WHAT IS CLAIMED IS:

1. A system for authenticating the identity of one of a plurality of individuals each having communication devices that are seeking access to at least one secure component having an input, the system comprising:

at least one record that includes information about each of the plurality of individuals, the information including a communication path which defines how to contact the individual's communication device and further defines a security protocol for allowing access to the secure component;

a controller having access to the at least one record wherein the controller receives signals from the input of the at least one secure component in response to the individual manipulating the input device, wherein the controller, in response to one of the individuals seeking access to the at least one secure component, retrieves the security protocol and the communications path from the at least one record; and

a communications interface that allows signals between the communications device carried by the individual and the controller wherein the controller (i) evaluates the signal received from the input device of the secure component, (ii) sends a first signal to the communications device of the individual in response to the individual seeking access to the at least one secure component and, (iii) evaluates a response signal by the individual by comparing the response signal to the security protocol to determine whether to allow access by the individual to the at least one secure component.

2. The system of Claim 1, wherein the security protocol comprises sending a prompt signal to the individual via the communications interface prompting the individual to enter and transmit an access code using the communications device and then comparing the access code to a pre-recorded access code stored in the at least one record to ascertain whether the individual correctly entered and transmitted the access code.

3. The system of Claim 2, wherein the at least one record further includes additional security criteria and wherein the controller allows access to the at least one secure component only when the individual has satisfied the security protocol and the additional security criteria.

4. The system of Claim 3, wherein the additional security criteria includes location information from which the individual must send the access code and wherein the individual's communication device transmits location information when transmitting the access code to the communications interface such that the controller can evaluate the additional security criteria.

5. The system of Claim 1, wherein the security protocol comprises sending an access code to the user via the communications interface and then evaluating whether the individual correctly entered the access code on the input of the at least one secure component.

6. The system of Claim 5, wherein the security protocol comprises (i) sending a prompt signal to the individual via the communications interface prompting the individual to enter and transmit a first access code using the communications device, (ii) comparing the first access code to a pre-recorded access code stored in the at least one record to ascertain whether the individual correctly entered and transmitted the first access code, (iii) sending a second access code to the communications device in response to determining that the individual correctly entered and transmitted the first access code, and (iv) evaluating whether the individual successfully entered the second access code on the input of the secure component before allowing access to the secure component..

7. The system of Claim 1, wherein the communications interface comprises a modem that is adapted to provide cellular telephone communication between the controller and cellular telephone devices carried by the plurality of individuals.

8. The system of Claim 1, wherein the at least one record further includes supplemental commands and corresponding actions wherein the controller, in response to receiving a supplemental command from a user, induces the system to implement the corresponding action.

9. The system of Claim 8, wherein the supplemental command comprises an additional access code provided to the controller via the communications interface by the individual communications device.

10. The system of Claim 9, wherein the supplemental command induces the controller to limit access to the at least one secure component.

11. The system of Claim 1, wherein the controller is adapted to remotely enable the secure component when the controller receives an enablement signal from the individual via the communications interface.

12. The system of Claim 11, wherein the controller remotely enables the secure component by sending a wake-on-LAN signal to the at least one secure component.

13. A system for allowing access of individuals having communication devices to one or more secure components having an input, the system comprising:

one or more records containing information about each individual, the information including a communication path as to how to contact the communication device for the individual and access codes for the individual;

a controller having access to the one or more records wherein the controller receives signals from the inputs of the one or more secure components wherein the controller, in response to one of the individuals seeking access to one of the secure components determines whether to allow access of the individual to the secure component;

a communications interface that permits communication between the controller and the communication device of the individual, wherein the controller receives an access code from the individual when the individual is seeking access to the secure component and compares the access code to the access code in the one or more records for the individual to determine whether to allow access such that access is allowed to the individual when (i) the individual has in their possession the communication device, (ii) provides the access code to the controller, and (iii) communicates to the controller via the input of the secure component.

14. The system of Claim 13, wherein the communication interface comprises a telephone modem that transmits signals to cellular telephones or cellular telephone enabled PDAs that comprise the communication devices of the individuals.

15. The system of Claim 13, wherein the access code is received by the controller via the individual's communication device via the communications interface.

16. The system of Claim 15, wherein the controller interfaces with the one or more secure components and wherein the one or more secure components includes an input such that signals entered on the input are received by the controller.

17. The system of Claim 16, wherein the controller is networked with the one or more secure components.

18. The system of Claim 16, wherein the access code is received by the controller via the input device of the secure component following the controller transmitting a prompt signal to the individual's communication device.

19. The system of Claim 18, wherein the prompt signal transmitted by the controller to the individual's communication device includes the access code the individual is to enter into the input device of the secure component.

20. The system of Claim 13, wherein the at least one record further includes supplemental commands and corresponding actions wherein the controller, in response to receiving a supplemental command from a user, induces the system to implement the corresponding action.

21. The system of Claim 20, wherein the supplemental command comprises an additional access code provided to the controller via the communications interface by the individual communications device.

22. The system of Claim 21, wherein the supplemental command induces the controller to limit access to the at least one secure component.

23. The system of Claim 13, wherein the controller is adapted to remotely enable the secure component when the controller receives a remote enablement signal from the individual via the communications interface.

24. The system of Claim 13, wherein the controller remotely enables the secure component by sending a wake-on-LAN signal to the at least one secure component.

25. A method of controlling access to a secure component of a system, the method comprising:

receiving a signal from an input of the secure component indicative of the individual seeking access to the secure component;

receiving an access code from an individual seeking access to the secure component;

comparing the access code to a stored access code;

communicating with the individual's portable communication device; and

allowing access to the secure component when the access code received from the individual matches the stored access code and when the individual has communicated with the system via their portable communication device.

26. The method of Claim 25, wherein communicating with the individual's portable communication device comprises sending cellular telephony signals to the individual's cellular telephone enabled device.

27. The method of Claim 25, wherein receiving the access code comprises receiving the access code from the individual's portable communication device.

28. The method of Claim 25, wherein receiving the access code comprises receiving the access code from the input of the secure component.

29. The method of Claim 25, further comprising:

receiving a supplemental command from the individual's communication device; and

implementing an action corresponding to the supplemental command.

30. The method of Claim 29, wherein implementing the action corresponding to the supplemental command comprises disabling portions of the secure component from access.